METHOD FOR PREVENTING ILLEGAL USE OF MOBILE COMMUNICATION TERMINAL

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a mobile communication terminal, and more particularly, to a method for preventing illegal use of a mobile communication terminal by a third party or a stranger.

2. Description of the Background Art

These days, thanks to its portability and convenience, a mobile communication terminal (referred to as 'terminal', hereinafter) is used by lots of people. The terminal provides various additional functions such as an address, a phone number, an itinerary management or a memo for a user's convenience.

If the terminal is lost with the various additional function provided, the user information stored in the corresponding terminal would be exposed as it is to a stranger. In order to prevent an illegal use of the lost terminal by a stranger, currently, various restriction functions such as a phone-locking function are provided to the terminal.

First, the user sets a phone-locking menu through a user interface, inputs a lock code to set a phone-locking state for the terminal.

Once the phone-locking state is set, the terminal is put in a state that it can only receive a call. Thus, even though the corresponding terminal is lost, the terminal is prevented from illegally using by a stranger and leakage of the user's

personal information can be prevented.

However, there has not been proposed any method for maintaining the user information and preventing an illegal use of a lost terminal by a stranger in case that a terminal is lost while its phone-locking function is not set.

Thus, in the past, if a terminal is lost while its phone-locking function is not set, there arises a problem that a stranger may use it illegally or leak the user information (an address, a phone number or a certain memo) stored in the terminal.

The above references are incorporated by reference herein where appropriate for appropriate teachings of additional or alternative details, features and/or technical background.

SUMMARY OF THE INVENTION

Therefore, an object of the present invention is to provide a method for preventing an illegal use of a mobile communication terminal that is capable of preventing or minimizing an illegal use of a lost terminal by a stranger from happening.

To achieve at least the above objects in whole or in parts, there is provided a method for preventing an illegal use of a mobile communication terminal including the steps of: transmitting a short message service (SMS) message to a lost terminal when a user requests a phone-locking service; and analyzing the SMS message by the lost terminal to set a phone-locking state or turn off a n LCD (liquid, crystal display) power.

To achieve at least these advantages in whole or in parts, there is further

provided a method for preventing an illegal use of a mobile communication terminal including the steps of: transmitting an SMS message to a lost terminal when a user requests a phone-locking service; checking whether a string contained in the SMS message is a ciphered string; comparing the ciphered string with a pre-set string to discriminate a type of the ciphered string, if the corresponding string is the coded .string; and setting a phone-locking state for the lost terminal or turning off the LCD according to the discriminated type of the ciphered string.

Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objects and advantages of the invention may be realized and attained as particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in detail with reference to the following drawings in which like reference numerals refer to like elements wherein:

Figure 1 is a schematic view of a mobile communication system adopted in the preferred embodiment of the present invention;

Figure 2 is a drawing illustrating a call processing for setting a phone-locking state for a lost terminal or turning off an LCD power in accordance with the preferred embodiment of the present invention;

Figure 3 is a drawing illustrating a format of an SMS message of Figure 2

in accordance with the preferred embodiment of the present invention; and

Figure 4 is a flow chart of a method for preventing an illegal use of a mobile communication terminal in accordance with the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is featured in that in case that a mobile communication terminal is lost in a state that its phone-locking function is not set, a short message service (SMS) message containing a ciphered string is transmitted to the lost terminal, to set a phone-locking state for the lost terminal or forcefully turn off an LCD power.

Figure 1 is a schematic view of a mobile communication system adopted in the preferred embodiment of the present invention.

As shown in Figure 1, when a terminal is lost, its user reports the loss of the terminal to an exchange 102, and at the same time, requests a phone-locking or an LCD power OFF service from the exchange 102 by using a terminal 100 or a public switched telephone network (PSTN) 105.

In response to the user's service request, the exchange 102 transmits an SMS message through a base station 103 to the lost terminal 104, and the lost terminal 104 analyzes the received SMS message to set a phone-locking function or turn off the LCD power.

The method for preventing an illegal use of a mobile communication terminal will now be described with reference to the accompanying drawings.

When the terminal is lost in a state that its phone-locking function is not

set, as shown in Figure 2, the user requests a phone-locking or an LCD power OFF service from the exchange 102 by using the terminal 100.

Upon receipt of the user's service request, as shown in Figure 3, the exchange 102 contains a ciphered string (##phone auto lock) into the SMS message and transmits it to the lost terminal 104 (step S2).

As the SMS message is received through the base station 103 from the exchange 102, the lost terminal 104 transmits a response message (Ack Message) to the base station 103 to acknowledge receipt of the message (step S3), and analyzes the received SMS message to turn off the phone-locking function or the LCD power.

In detail, as shown in Figure 4, when the SMS message is received, a software of the lost terminal 104 analyzes the received SMS message and check whether a ciphered string exists in the SMS message (step S12). In this respect, the ciphered string is discriminated by '##' and a phone auto lock indicates a lock code or a power-OFF code.

If a ciphered string (##) is contained in the SMS message, the software discriminates whether the corresponding ciphered string is for a phone-locking use or for the LCD power-OFF use (step S13). The discrimination is made by comparing the code value (the lock code or the power-OFF code) of the received ciphered string and an internal string set by the user or an existing string.

If a string contained in the SMS message is not a ciphered string, the software performs a processing of a general SMS message likewise in the conventional art.

Once the type of the ciphered string is discriminated, the software of the lost terminal 104 drives a hardware according to the discriminated ciphered string

type, to set a phone-locking function or turn off the LCD power (step S14).

For example, in the step S13, if the ciphered string is for a phone-locking use, the software reads a lock code for setting a phone-locking from a non-volatile memory (not shown). And then, the software enables a variable value for setting a phone-locking, sets other related codes and sets a phone-locking for the lost terminal 104. And then, the software finally displays the phone-locking state on the LCD screen.

Accordingly, so long as the stranger is not aware of the lock code, he or she may not use the lost terminal 104 or leak the user's personal information.

In the step S13, if the ciphered string is for the LCD power-OFF use, the software disables a regulator drive signal outputted to a general purpose input/output (GPIO) port of a mobile station modem (MSM) (not shown) and enables its related data variable of a non-volatile memory. The variable is to prevent the power of the LCD to be driven when the power is again turned on. Resultantly, a regulator (not shown) which supplies the LCD power (Vcc) according to the drive signal is disabled, so that the power supply (Vcc) to the LCD is cut off.

Accordingly, though the lost terminal is turned on, since the screen of the LCD is turned off, the stranger may not read or leak the user's personal information stored in the lost terminal 104.

Thereafter, when the user gets back the lost terminal 104, he or she can re-operate the OFF LCD by inputting a string of '##LCDON' and clearing again the data of the non-volatile memory.

As so far described, the method for preventing illegal use of a mobile communication terminal has the advantage that, when a terminal is lost, an SMS

message containing a ciphered string is transmitted to the lost terminal to set a phone-locking or forcefully turn off an LCD power, so that the lost terminal can be prevented from illegally using by a third party or a stranger and user's personal information can be effectively prevented from leaking.

The foregoing embodiments and advantages are merely exemplary and are not to be construed as limiting the present invention. The present teaching can be readily applied to other types of apparatuses. The description of the present invention is intended to be illustrative, and not to limit the scope of the claims. Many alternatives, modifications, and variations will be apparent to those skilled in the art. In the claims, means-plus-function clauses are intended to cover the structure described herein as performing the recited function and not only structural equivalents but also equivalent structures.